

The Impersonation Economy

Copyright Pretexts, Synthetic Identity, Account Markets and Social-Media Scam Supply Chains

An evidence review, investigative framework and public-interest response guide, 2020–2026

ABDUL QUDOOS

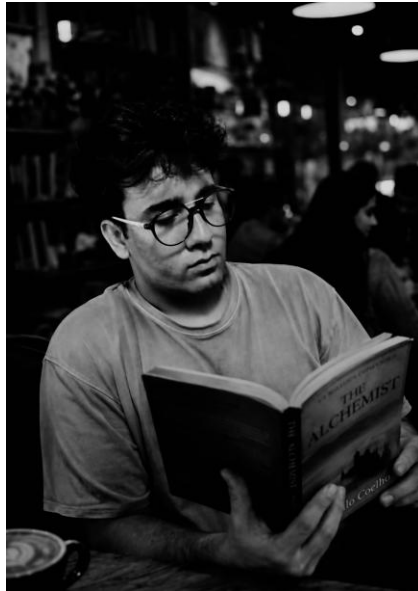
Independent Researcher and Investigator | Lahore, Pakistan

RESEARCH CUT-OFF

10 August 2026 | Version 2.0

ORIGINAL CONTRIBUTION The Trust-Asset Stack, an attribution protocol, a loss-accounting model and an incident-level evidence schema for studying copyright-pretext impersonation without manufacturing a headline market value.

© 2026 Abdul Qudoos. Independent working paper; not peer reviewed.



PUBLICATION NOTE

This report is an independent public-interest research paper. It synthesizes official statistics, legislation, court and enforcement records, platform disclosures, academic research and carefully labelled secondary reporting available through 10 August 2026. It has not been peer reviewed, commissioned by a platform or endorsed by any government agency. Legal discussion is general information, not legal advice.

Abdul Qudoos is an independent researcher and investigator based in Lahore, Pakistan. He reports approximately ten years of experience examining corporations, online markets, scams and manipulation, including one year focused on copyright-pretext impersonation and its enabling markets. That experience statement is supplied by the author and has not been independently audited. The one-year observations helped define the questions and categories in this paper; because no coded field dataset or transaction ledger accompanies this edition, they are not used to calculate prevalence, revenue or loss.

ACKNOWLEDGMENT AND BOOK CREDIT

The author acknowledges Ans Ishfaq’s 2025 book Digital Fortress as a practical influence on the creator-defence portions of this report—especially its emphasis on asset inventories, account security, evidence preservation, monitoring, lawful takedown processes and repeatable incident response. The book is used here as a practitioner framework, not as the sole authority for empirical, legal or statistical claims; those claims are independently sourced.

Bibliographic transparency matters. The supplied PDF is titled Digital Fortress: The Creator’s Guide to Securing Content, Brand, and Legal Rights in the Online World and says it was first published in 2025, but its visible title and copyright pages do not print an author name. Contemporary publication profiles attribute a matching 110-page Digital Fortress volume to Ans Ishfaq. This report credits Ishfaq on that basis and advises confirming the final publisher or retail metadata before submission to a journal or library catalogue.

SUGGESTED CITATION Qudoos, A. (2026). The Impersonation Economy: Copyright Pretexts, Synthetic Identity, Account Markets and Social-Media Scam Supply Chains (Version 2.0). Independent research report.

EVIDENCE LANGUAGE USED THROUGHOUT

Label	Meaning	Publication rule
Established	Supported by an official record, audited filing, statute, court disposition or multiple convergent primary sources.	State the source, period, jurisdiction and exact category.
Platform-reported	Disclosed by the platform about its own systems or enforcement.	Attribute to the platform; do not convert removals into prevalence or victim counts.
Alleged	Appears in a complaint, indictment or unresolved enforcement action.	Use allegation language and identify the procedural status.
Reported	Published by a credible news organization or other secondary source.	Identify the original evidence where possible and disclose disputes.
Field observation	Observed or described by the author but not represented by a reproducible coded dataset in this edition.	Use to form hypotheses, not monetary totals or prevalence claims.

ABSTRACT

Social-media impersonation is not a single offence, platform or marketplace. It is a supply chain that can combine stolen or purchased accounts, copied creative assets, synthetic identity documents, fabricated authority, deceptive advertising, private-message migration, payment extraction and laundering. Copyright appears in three distinct roles: protected content is copied to make a false profile credible; real notice-and-takedown systems are abused to pressure or silence a target; and fake “copyright strike” or platform-support messages are used as social-engineering pretexts to steal credentials, account control or money. Treating all three as one category of “copyright fraud” hides both the legal distinctions and the measurable harms.

This report reviews evidence available through 10 August 2026. U.S. consumers reported about \$2.1 billion in 2025 losses from fraud for which social media was the identified contact method, up from \$261 million in 2020. In a separate series, the Federal Trade Commission reported \$3.5 billion in losses to imposter scams across contact methods in 2025. The FBI’s Internet Crime Complaint Center received 1,008,597 complaints involving \$20.877 billion in reported loss in 2025. Those figures demonstrate scale but are neither global nor specific to copyright-pretext impersonation. Broader enforcement records show industrial enabling markets: Genesis Market commodified account access; U.S. actions against VerifTools and OnlyFake documented services producing counterfeit identity documents; Meta reported removing 159 million scam advertisements, 10.9 million scam-centre-linked accounts and more than 20 million accounts impersonating large creators during 2025; and UNODC and INTERPOL describe transnational scam centres, marketplaces and identity fraud at regional and global scale.

The report’s central conclusion is deliberately precise: the enabling ecosystem is large, transnational and commercially organized, but no credible public dataset establishes an exact global loss or revenue value for the narrow market of copyright-pretext social-media impersonation. The original contribution is therefore methodological. The report proposes a Trust-Asset Stack, separates location signals into attribution planes, introduces a non-additive loss-accounting model, and supplies an Impersonation Incident Record for future research in Pakistan and internationally.

Keywords: *social-media fraud; impersonation; account takeover; copyright abuse; synthetic identity; account markets; Telegram; social engineering; Pakistan; platform governance*

EXECUTIVE FINDINGS

1. The object being traded is transferable trust. A mature identity, recognizable content, established account history, platform authority and believable payment path can be bought, stolen, forged or imitated separately, then assembled into one persuasive front.
2. Copyright is a high-leverage pretext because creators know that real strikes and removals can interrupt income or endanger account continuity. The scammer borrows that real institutional fear, then redirects the target to a false login, false agent, payment demand or account-recovery step.
3. The strongest public channel statistic is the FTC’s approximately \$2.1 billion in U.S. reported 2025 losses where social media was the identified contact method. It is broader than impersonation, incomplete by design and not a global estimate.
4. No public filing shows how much Meta lost—or earned—specifically from fake copyright scams. Meta’s 2025 total revenue was \$200.966 billion, but its audited filings do not isolate scam-ad revenue, copyright-pretext revenue, victim loss or attributable integrity cost.

5. Reuters reported that internal Meta documents estimated about 10.1% of 2024 revenue—roughly \$16 billion—from scams and prohibited goods. Meta called the estimate rough and overly inclusive. A 2026 Santa Clara County complaint separately alleges about \$7 billion in annual revenue from ads exposing users to scams. Neither number is an audited finding about copyright impersonation; the complaint remains unresolved.
6. Access and synthetic verification are demonstrably commodified. Genesis Market offered more than 80 million account-access credentials tied to more than 1.5 million compromised computers. Later U.S. actions described counterfeit licence and passport services intended to bypass online identity checks and obtain accounts.
7. Advertisements for bans, unbans, verification and account recovery must be coded cautiously. A seller's listing proves only that a service was advertised. It does not prove delivery, platform insider access, the truth of the claimed method or a completed transaction.
8. Telegram can act as a discovery, coordination and migration layer, but it is not the whole market. Telegram's dynamic safety counter and UNODC's observations of underground markets establish an enforcement and marketplace burden, not a transaction-value census.
9. Geographic attribution is routinely overstated. Victim location, phone registration, payment beneficiary, server location, account login, marketplace language, workforce location and organizer control are different evidence fields. None should silently substitute for another.
10. Pakistan has relevant law and reporting channels under the Prevention of Electronic Crimes Act, the Copyright Ordinance, NCCIA and PTA, but no comparable public national loss series for this niche was located. A Pakistan-centred, incident-level dataset would be a genuine public contribution.
11. Durable disruption must be measured beyond takedowns: re-registration time, repeat-victim contact, administrator overlap, payment migration, domain replacement and restoration of legitimate accounts are better indicators of whether an operation was actually disabled.

CONTENTS

1. Purpose, contribution and research questions
 2. Method, positionality and evidentiary standard
 3. Scope and terminology
 4. The Trust-Asset Stack
 5. How the market works: a modular supply chain
 6. The art of manipulation
 7. Account markets, synthetic identity and verification claims
 8. Telegram and the marketplace layer
 9. What the numbers establish—and what they do not
 10. Meta fact-check: revenue, losses, enforcement and allegations
 11. Copyright, impersonation and legal-process abuse
 12. Evidence-based case studies
 13. Impact on creators, consumers, platforms and society
 14. Pakistan focus and comparative research gaps
 15. Recommendations
 16. Measurement framework for future field research
 17. Limitations and conclusion
- Appendix A. Claim audit and evidence matrix
- Appendix B. Impersonation Incident Record
- Appendix C. Public incident-response checklist
- References

1. PURPOSE, CONTRIBUTION AND RESEARCH QUESTIONS

The study explains how impersonation operations acquire credibility, reach targets, convert attention into money or account control, and recycle infrastructure. It focuses on schemes that impersonate creators, companies, platform personnel, lawyers, public officials or other trusted identities, including schemes that use copyright language as a threat, lure or procedural weapon.

The paper makes a narrower and more defensible contribution than a claim to have discovered the global value of an underground market. It connects previously separated evidence—fraud loss reports, account-access markets, synthetic identity services, platform enforcement, copyright process design and social-engineering research—into a single analytical model. It then identifies the exact incident fields needed to test that model prospectively.

RESEARCH QUESTIONS

12. Which trust assets are copied, stolen, purchased, rented or fabricated in an impersonation operation?
13. How are those assets assembled into a supply chain across social networks, messaging services, domains, ad systems and payment rails?
14. What role does copyright play as copied property, as a real but abused legal process, and as a fabricated platform pretext?
15. Which public numbers are reliable, what precisely do they measure, and which combinations would produce double counting or false precision?
16. How should Telegram, account markets, synthetic IDs, verification offers, ban/unban services and claimed insider access be studied without advertising live criminal access points or accepting vendor claims as fact?
17. How can researchers describe geography without confusing infrastructure, payment, language, victim and organizer signals?
18. What evidence would permit a responsible Pakistan-centred estimate of incidence and verified loss?

RESEARCH BOUNDARY This report is defensive and non-operational. It does not identify active vendors, publish invite links, reproduce access instructions, buy illegal access, test stolen credentials or teach evasion of platform controls.

2. METHOD, POSITIONALITY AND EVIDENTIARY STANDARD

2.1 DESIGN

This is a structured secondary-evidence review and conceptual synthesis. Sources were collected through the research cut-off and grouped into five classes: official statistics and legal records; platform disclosures; peer-reviewed or university research; high-quality investigative reporting; and author field observations. Highest evidentiary weight is assigned to original records. Secondary reporting is used when it describes non-public documents or supplies context that cannot be independently reproduced, and disputes are retained rather than resolved by assertion.

Quantitative claims were retained only when the source, period, geography, unit and category could be stated together. Each headline number was tested against four questions: Is it reported or modelled? Does it count incidents, accounts, ads, complaints, transactions

or dollars? Can categories overlap? Does the source cover the narrow phenomenon studied here? This process led to the exclusion of any exact global market value for copyright-pretext impersonation.

Grade	Evidence type	Use	Principal limitation
A	Official statistics, statutes, court records, audited filings, regulator or enforcement releases	Core legal and quantitative claims	Underreporting, category overlap, jurisdictional limits and allegations before disposition
B	Original platform transparency, safety or threat reports	Platform-scale enforcement and observed tactics	Self-reported; definitions and detection coverage vary
C	Peer-reviewed or university research	Mechanisms, samples and analytical models	Observation windows or platforms may be narrow
D	Investigative journalism and reputable technical reporting	Non-public documents, disputed claims and leads	Dependent on source access; not an audited filing
E	Author observations and marketplace advertisements	Hypothesis generation and category design	Seller deception, selection bias and no reproducible sample in this edition

2.2 ANTI-ERROR RULES

19. A complaint count is not an estimate of all incidents. People may not recognize, report or correctly categorize fraud.
20. A takedown count is not an estimate of all active accounts or unique offenders. One actor may control many accounts; one account may be removed more than once or replaced.
21. An advertisement, channel post or vendor price is not proof of inventory, capability, sale, revenue or platform insider access.
22. Broad loss series must not be added to one another when they overlap in victims, time, geography or category.
23. Attempted loss, paid amount, recovered amount, seller revenue, platform revenue and social cost are different measures and remain separate.
24. A complaint or indictment establishes allegations. A plea, verdict, final judgment or verified seizure supports a different level of claim.

2.3 POSITIONALITY, ETHICS AND REPRODUCIBILITY

The author approaches the subject as an independent investigator in Lahore, with practical interest in corporate accountability, scam markets and manipulation. That position provides useful pattern recognition but can also create confirmation risk: dramatic marketplace claims are easy to notice, while failed or fraudulent vendors and incidents that never reach investigators are less visible. The report therefore separates field-informed hypotheses from externally verifiable findings.

Ethical limits include minimization of personal data, no publication of live criminal endpoints, no purchase or testing of stolen credentials, no direct contact that increases victim risk, and protection for persons trafficked or coerced into scam-centre labour. A later empirical study should preregister its codebook, preserve time-stamped source captures, document inclusion and exclusion criteria, and publish an anonymized data dictionary even when the underlying evidence cannot be released.

3. SCOPE AND TERMINOLOGY

Term	Working definition
Identity impersonation	A false representation that an account, message, service or offer is controlled or authorized by a real person or organization.
Content cloning	Copying photographs, video, posts, biographies, design assets or other expression to manufacture resemblance and credibility.
Account takeover	Unauthorized control of an existing account through stolen credentials, session tokens, malware, compromised recovery channels or social engineering.
Aged or cultivated account	An account with accumulated history, followers, engagement or reputation signals that may appear more credible than a new profile.
Copyright pretext	A false or misleading claim about infringement, a strike, a takedown or platform authority used to create fear, urgency or compliance.
False copyright complaint	A notice submitted without a valid basis, or with a knowing material misrepresentation, to remove content, redirect monetization or pressure a target.
Synthetic identity artifact	A fabricated or altered identity document, selfie, video, profile or data package used to pass a verification check or support a false identity.
Access market	A marketplace or broker that sells credentials, session access, device fingerprints, malware-derived profiles or control of online accounts.
Impersonation marketplace	The distributed set of sellers, brokers, access providers, channels, hosting services, ad accounts, payment intermediaries and laundering services enabling impersonation.
Scam centre	An organized operation using labour, scripts, technical systems and payment infrastructure to conduct fraud at scale; documented centres may also involve trafficking and forced criminality.

Three boundaries are essential. First, copying a creator’s photograph can be a copyright issue, while pretending to be the creator is primarily an identity and fraud issue and may also involve trademark, passing off, privacy or publicity law. Second, a forged “copyright strike” email is social engineering unless a real legal notice was filed. Third, account recovery or rights-enforcement services can be legitimate; the risk arises where identity, authority, access, outcomes or platform affiliation are misrepresented.

4. THE TRUST-ASSET STACK

The proposed Trust-Asset Stack explains why a copied profile can become more dangerous when combined with other assets. The scammer does not need to be the original creator, own the account, operate the ad campaign, manufacture the identity document and receive the payment. Each asset can be sourced separately. The finished impersonation is persuasive because the victim sees a coherent surface while the underlying components come from different suppliers.

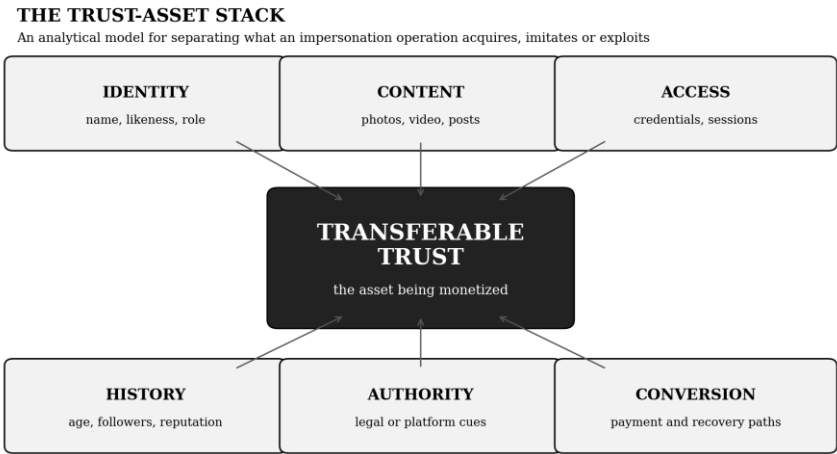


Figure 1. The Trust-Asset Stack. Original analytical model developed for this report.

Trust asset	How it is acquired or imitated	Evidence to preserve	Priority control
Identity	Copied name, likeness, biography, role, voice or relationship	Source profile; copied media; account ID; naming history	Official-account directory; similarity detection; impersonation reporting
Content	Downloaded posts, livestream clips, brand graphics or AI-generated derivatives	Original file; publication date; licence or ownership record; hashes	Watermark/provenance where appropriate; media matching; lawful enforcement
Access	Phishing, malware, token theft, compromised recovery or purchased credentials	Login alerts; active sessions; recovery changes; malware findings	Passkeys or hardware-backed MFA; device-bound sessions; rapid revocation
History	Aged account, purchased audience, renamed profile or coordinated engagement	Creation date; rename history; follower pattern; archived views	High-risk rename controls; account-history signals; re-verification
Authority	Fake legal notice, support role, verified-style badge, forged letter or synthetic ID	In-product case record; message headers; document metadata; sender domain	Signed in-product notices; independent contact verification; staff identity controls
Conversion	Bank, wallet, payment link, recovery fee, ad offer or credential capture	Payment request; beneficiary; receipt; redirect chain; wallet address	Step-up payment warnings; beneficiary intelligence; freezes and recovery

Sources: Original synthesis informed by U.S. DOJ (2023, 2025, 2026), Europol (2025), Google TAG (2021), FBI (2024) and Stajano and Wilson (2011).

ANALYTICAL IMPLICATION Enforcement that removes only the visible profile leaves the supplier network intact. Durable intervention traces administrator overlap, stolen access, synthetic verification, domains, ad buyers, payment beneficiaries and replacement accounts.

5. HOW THE MARKET WORKS: A MODULAR SUPPLY CHAIN

The lifecycle below is a synthesis, not a claim that every operation uses every stage. Its value is diagnostic: each stage leaves different evidence, involves different service providers and requires a different intervention. The person messaging the victim may be only the conversion operator, not the party who stole the account or controls the proceeds.

Stage	Function	Typical evidence	Defensive intervention
-------	----------	------------------	------------------------

Stage	Function	Typical evidence	Defensive intervention
1. Targeting	Select a creator, brand, executive, community or victim segment with transferable trust.	Look-alike searches, copied-asset alerts, repeated profile viewing or contact patterns	Verified contact directory; monitoring; creator and staff education
2. Asset acquisition	Obtain content, credentials, session access, synthetic identity artifacts or an aged account.	Malware alert, session anomaly, document metadata, market seizure record	Passkeys; device-bound sessions; recovery security; document verification
3. Credibility manufacture	Add history, followers, comments, copied posts, verification-like cues or fabricated support material.	Burst growth, reused media hash, renamed account, coordinated engagement	Rename and age signals; similarity detection; engagement integrity
4. Distribution	Reach targets through ads, search, comments, direct messages, fake support or hijacked audiences.	Ad library record, referrer, message header, campaign URL, account cluster	Advertiser verification; link-risk warnings; network detection
5. Migration	Move the conversation from a public platform to a private channel, website, email, phone or messenger.	Invite URL, redirect chain, contact handle, timestamped conversation export	Contextual warnings; friction for risky links; cross-platform referrals
6. Manipulation	Use authority, urgency, scarcity, fear, social proof, helpfulness or promised gain.	Scripts, repeated wording, fake testimonials, legal language, payment deadline	Cooling-off periods; in-product verification; independent confirmation
7. Conversion	Collect credentials, account control, codes, fees, deposits, cryptocurrency or identity data.	Login and recovery events, receipt, wallet, mule account, uploaded document	Payment holds; step-up verification; rapid session and transfer response
8. Laundering and recycling	Move proceeds, sell access again, rename accounts, redeploy domains or retarget victims with recovery scams.	Shared beneficiaries, wallet cluster, domain reuse, device/admin overlap	Asset freeze; infrastructure seizure; repeat-victim protection; disruption metrics

5.1 WHAT AN ILLICIT LISTING CAN—AND CANNOT—PROVE

Author observations describe offers for aged accounts, account access, followers, verification, bans and unbans, synthetic IDs and rights-enforcement services. Such listings are relevant as market signals, but criminal markets also contain duplicate inventory, recycled screenshots, fake escrow, fabricated testimonials and vendors who scam other offenders. The minimum unit of evidence is therefore not the screenshot alone. A credible case requires a stable listing identifier, archived timestamp, seller history, transaction evidence, delivery evidence, post-sale control and—where money is measured—a verified payment flow.

Claims of “inside access” require still stronger proof. A successful unban may result from ordinary appeal, timing, compromised agency access, social engineering, bribery, stolen staff credentials or pure coincidence. Researchers should code the seller’s claim separately from the observed outcome and should never infer a platform employee relationship from advertising language alone.

6. THE ART OF MANIPULATION

Technical access creates opportunity; manipulation produces compliance. The “art” is not mystical. It is the disciplined arrangement of credible cues around a request the target would normally reject. Stajano and Wilson’s systems-security analysis of scams identifies recurring principles including social compliance, time pressure, herd behaviour, distraction, need or greed, kindness and the victim’s reluctance to admit a questionable choice. Copyright pretexts add a particularly effective institutional cue: creators already know that real rights complaints can affect reach, monetization and account survival.

Manipulation principle	Copyright/impersonation application	Design response
Authority and social compliance	A fake platform employee, lawyer, executive or known creator demands action.	Show verified staff and legal notices inside the product; confirm through independently obtained channels.
Urgency and time	A strike, account closure or limited opportunity supposedly requires immediate login, payment or code sharing.	Cooling-off periods; persistent warnings; no deadline-based loss of appeal rights where feasible.
Social proof and herd	Followers, comments, testimonials, mutual contacts or verification-like graphics imply acceptance.	Expose rename history, account age and suspicious engagement; warn on copied-profile similarity.
Distraction	Legal language or a brand deal absorbs attention while a link captures credentials or malware is delivered.	Separate case review from login; show destination domains and file-risk warnings.
Need, greed and fear	Recovery, investment returns, grants, refunds, account preservation or reputation protection are conditional on payment.	Transaction warnings, payment holds, trusted recovery channels and clear escalation.
Kindness and reciprocity	The actor first offers help, promotion or collaboration, then requests access or money.	Independent verification before delegation; least-privilege collaborator access.
Commitment and shame	After a small payment or disclosure, the victim is pressured to continue or avoid reporting.	Normalize rapid reporting, nonjudgmental support and repeat-victim warnings.

6.1 THE COPYRIGHT-PRESSURE SEQUENCE

- 25. Borrow real institutional language: strike, infringement, counter-notice, legal department, monetization hold or suspension.
- 26. Create a countdown or consequence that narrows attention and discourages independent verification.
- 27. Present a false resolution path: external form, private agent, remote-support call, downloadable evidence file or payment address.
- 28. Capture the asset actually sought: credentials, session token, recovery code, identity document, account role or money.
- 29. Exploit the compromised account or sunk cost, then recycle the identity against followers or return as a recovery service.

CLASSIFICATION RULE Record copied content, identity impersonation, fake platform communication, real-process abuse, account takeover and payment fraud as separate acts even when they occur in one incident. This prevents ‘copyright fraud’ from becoming an unusably broad category.

7. ACCOUNT MARKETS, SYNTHETIC IDENTITY AND VERIFICATION CLAIMS

7.1 ACCOUNT ACCESS AS A COMMODITY

The dismantling of Genesis Market provides strong official evidence for an industrial access layer. U.S. authorities described a marketplace that sold usernames, passwords, session information and device fingerprints obtained from malware-infected computers. At the time of disruption, authorities reported more than 80 million account-access credentials associated with more than 1.5 million compromised computers; social-media access was among the available data types. The figures establish inventory at scale, not completed purchases, unique impersonation cases or seller revenue.

Europol’s 2025 Internet Organised Crime Threat Assessment describes a wider “steal, deal, repeat” cycle in which compromised data and access are traded and reused. The

important inference is organizational: the downstream impersonator does not need to write malware. Access brokers, infostealer operators, credential markets and account sellers can supply control as a service.

7.2 SYNTHETIC DOCUMENTS AND VERIFICATION

Official U.S. actions in 2025 and 2026 support the existence of commercial synthetic-identity services. In August 2025, the Justice Department announced the seizure of VerifTools marketplace domains and stated that the service sold counterfeit driver’s licences and passports used to bypass identity-verification systems and gain unauthorized access to online accounts. In February 2026, the creator of OnlyFake pleaded guilty in a case involving the sale of more than 10,000 digital fake identity documents purporting to come from 56 countries. An earlier SecondEye prosecution described false documents marketed for creating accounts at banks, payment services, social networks and digital-currency platforms; advertisements also claimed an ability to help banned or suspended users regain access.

These cases support a market category, not a universal success rate. Verification systems differ by platform and evolve; a generated image that looks plausible to a person may fail automated checks, and a seller may falsely claim acceptance. The FBI separately warns that generative AI can create profile images, identification documents and other materials used to make a fraudulent identity persuasive. Researchers should record the document type, claimed jurisdiction, verification target, observed result and official case status rather than treating “AI ID” as a single capability.

Advertised service	What the advertisement proves	Evidence required for a stronger conclusion
Aged or high-follower account	A seller represented that such an account was available.	Stable account ID, provenance, seller control, completed transfer, post-sale control and replacement risk
Verification or synthetic ID	A document or outcome was offered or displayed.	Document provenance, target workflow, time-stamped result, platform response and absence of recycled evidence
Ban/unban or recovery	A seller claimed a restoration capability.	Case ID, starting status, exact action, final status, timing, ordinary appeal history and independent confirmation
Copyright strike or removal	A seller offered reporting or legal-process action.	Notice record, claimed rightsholder, protected work, platform case, outcome and validity assessment
Platform insider	The seller used an authority claim.	Verified employment or contractor relationship, access logs, communications and adjudicated evidence; never infer from success alone

Sources: U.S. Department of Justice actions concerning Genesis Market (2023), SecondEye (2021), VerifTools (2025) and OnlyFake (2026); FBI generative-AI warning (2024).

PUBLIC-SAFETY RULE Do not test a vendor with a real account, stolen credential, forged identity or fraudulent notice. Defensive research can establish market structure through archived advertisements, court records, victim evidence, platform outcomes and financial records without increasing harm.

8. TELEGRAM AND THE MARKETPLACE LAYER

Telegram can serve several functions at once: public discovery, private negotiation, group coordination, bot-mediated interaction, customer support, reputation signalling and migration from another platform. UNODC’s research on Southeast Asian organized crime

reviewed hundreds of regionally focused Telegram underground markets and forums and described specialized services linked to cyber-enabled fraud, underground banking, stolen data and technical infrastructure. The defensible conclusion is that Telegram is an important layer in parts of the ecosystem—not that it is the only market or the cause of every transaction.

A market can begin on a search engine or social-media advertisement, move to Telegram for conversation, use a web panel for delivery and finish through a bank, wallet or mule network. Conversely, public-channel observation can badly overstate activity: channels may be duplicated, abandoned, inflated with fake members, infiltrated, repurposed after enforcement or fraudulent toward their own buyers.

Evidence	What it supports	What it does not support
Telegram Safety Overview displayed more than 22.5 million groups and channels blocked during 2026 when observed on 10 August 2026.	A very large moderation workload across the service and a time-stamped platform claim.	A scam-only count, unique offenders, marketplace revenue or the total number of harmful communities.
Telegram’s EU DSA guidance prohibits public illegal-goods offers including forged documents and states that impersonating or defrauding accounts may be labelled FAKE or SCAM, blocked or deleted.	Formal recognition of impersonation, fraud and forged-document risks in platform policy.	An audit of enforcement completeness, accuracy, appeal quality or private activity.
UNODC observed hundreds of regionally focused Telegram markets and forums in its wider study of Southeast Asian organized crime.	A marketplace and coordination role within a transnational ecosystem.	A global census, proof that every listing is real or proof that Telegram alone enabled the crime.
A victim conversation migrated to Telegram.	One incident’s communication path.	The offender’s nationality, the server location, the payment controller or the origin of the scheme.

Sources: *Telegram Safety Overview and EU DSA guidance (accessed 10 August 2026); UNODC, Inflection Point (2025).*

8.1 A NON-AMPLIFYING MARKETPLACE RESEARCH PROTOCOL

- 30. Collect public evidence with a research identifier and UTC timestamp; preserve screenshots, URLs and channel identifiers without republishing live access links.
- 31. Code the advertised product, price, currency, audience size, seller claim, payment method and proof type separately.
- 32. Deduplicate mirrored channels, reposts, seller aliases and repeated inventory using identifiers, media hashes and text similarity.
- 33. Distinguish public discovery, private negotiation, delivery interface and payment rail. Do not attribute all stages to Telegram.
- 34. Record whether a listing disappeared, was labelled, migrated, reappeared or changed administrators; takedown durability is an outcome variable.
- 35. Never publish stolen data, live credentials, personal identity documents, criminal invitations or operational evasion details.

9. WHAT THE NUMBERS ESTABLISH—AND WHAT THEY DO NOT

Public statistics are strongest when used at their stated level. The FTC series measures reports to the U.S. Consumer Sentinel Network in which social media was the identified contact method. The FBI IC3 series measures complaints submitted to a U.S. reporting programme. UNODC’s regional figure is a modelled estimate for all scams across a

defined group of countries. INTERPOL and Meta report enforcement activity. These sources illuminate different layers and must not be summed into one market value.

U.S. reported losses where social media was the contact method

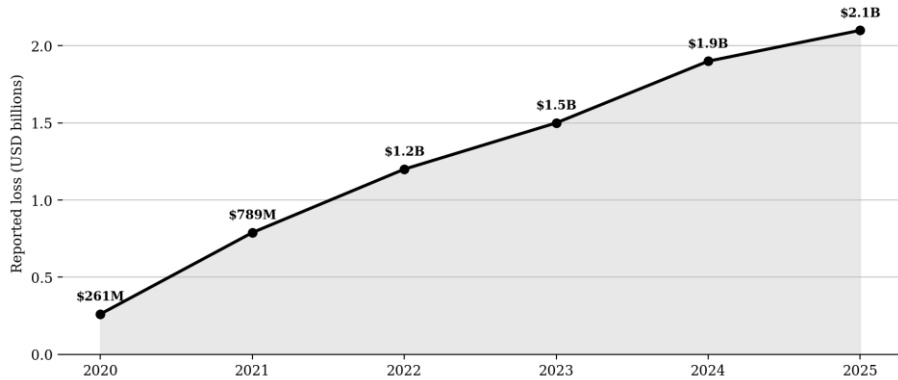


Figure 2. FTC Consumer Sentinel reported losses where social media was the identified contact method, 2020–2025. Values are rounded as published; voluntary reports do not represent all losses, and collection was interrupted during the 2025 U.S. government shutdown.

Indicator	Period / geography	Published value	Correct interpretation
FTC: fraud where social media was contact method	2025; U.S. reports	\$2.1B reported loss; social media named in 28% of loss reports with a known standard contact method	Channel-level reported loss; broader than impersonation and not global
FTC: imposter scams across contact methods	2025; U.S. reports	\$3.5B reported loss; nearly one in three fraud reports	Broad scam type across channels; cannot be added to the social-media figure
FBI IC3: all internet crime	2025; complaints to IC3	1,008,597 complaints; \$20.877B reported loss	Broad reporting programme, not social-media-only; categories may overlap
FBI IC3: cyber-enabled fraud	2025; complaints to IC3	452,868 complaints; \$17.697B reported loss	A broad subset: 45% of complaints and 85% of reported loss
FBI IC3: government impersonation	2025; complaints to IC3	32,424 complaints; \$797.9M reported loss	One impersonation subtype; excludes creator, brand and support impersonation
FBI IC3: IPR/copyright/counterfeit	2025; complaints to IC3	2,386 complaints; \$26.7M reported loss	An intellectual-property category, not all copyright-pretext fraud
FBI IC3: AI-related descriptor	2025; complaints to IC3	22,364 complaints; \$893.3M reported loss	Descriptor-based count across crime types; not proof that AI caused every loss
UNODC regional scam estimate	2025; East/Southeast Asia, Australia and New Zealand	\$88.3B–\$114.1B estimated scam loss	All scams in the stated region; modelled and not social-media- or impersonation-only
INTERPOL Operation First Light	2026; 97 countries	5,811 arrests; \$293M intercepted	Enforcement outcome across social-engineering fraud types; not market revenue
Meta enforcement disclosure	2025; global	159M scam ads; 10.9M accounts linked to criminal scam centres	Platform detections/removals; not unique offenders, victims or loss
Meta large-creator impersonation disclosure	2025; global	>20M accounts removed	Platform-defined enforcement count; not successful scams or perpetrators

Sources: *U.S. FTC (2026a, 2026b); FBI, 2025 IC3 Annual Report (2026); UNODC (2026); INTERPOL (2026); Meta (2026a, 2026b).* Categories and methods differ and must not be summed.

9.1 WHY AN EXACT GLOBAL NICHE VALUE IS NOT SUPPORTABLE

A credible estimate needs a defined population, observed numerator, defensible denominator and tested coverage assumptions. The narrow niche currently has none of these at global scale. Complaint data omit unrecognized and unreported events; platforms apply different categories; law-enforcement actions are selected cases; marketplace listings are duplicated and frequently deceptive; wallet flows can combine unrelated activity; and one incident may appear in several datasets.

The phrase “market worth” is also ambiguous. It may refer to money paid by victims, gross advertiser spend, revenue earned by criminal suppliers, the resale price of accounts, attempted loss, recovery cost or broader social harm. Those quantities have different units and owners. A publication that mixes them can produce a large number that is mathematically impressive and scientifically meaningless.

PUBLICATION-SAFE CONCLUSION Available evidence establishes a large and industrialized enabling ecosystem, but it does not establish an exact global dollar value for copyright-pretext social-media impersonation. ‘Billions’ is a defensible broad fraud-loss context, not a measured value of this niche.

9.2 LOSS ACCOUNTING WITHOUT DOUBLE COUNTING

Measure	Definition	Treatment
Amount requested	Money the actor demanded or attempted to capture	Report separately; never call it loss unless paid
Gross paid amount	Money transferred by the victim	Verify through receipt, bank or wallet record
Recovered amount	Money returned, reversed, frozen or otherwise restored	Subtract from gross paid amount for net verified victim loss
Creator interruption loss	Verified income lost during account or content disruption	Document baseline and period; disclose assumptions
Recovery and remediation cost	Professional fees, incident-response labour and necessary replacement costs	Use receipts or documented labour method; keep separate from transfer loss
Platform or intermediary cost	Attributable review, refund, investigation, support or infrastructure expense	Usually unavailable publicly; do not infer from company revenue
Criminal supplier revenue	Verified receipts earned for accounts, documents, ads, access or services	Requires transaction-level evidence and seller deduplication

CORE EQUATION Net verified victim loss = gross paid amount – recovered amount. Other costs may be reported alongside it, but only after incident-level deduplication and explicit methods; attempted amounts remain separate.

10. META FACT-CHECK: REVENUE, LOSSES, ENFORCEMENT AND ALLEGATIONS

The question “How much did Meta lose through fake copyright scams?” has no supported public numerical answer. Meta’s audited 2025 filing reports \$200.966 billion in total revenue, \$117.690 billion in costs and expenses, and \$60.458 billion in net income. The filing discusses investments and risks related to platform integrity, deceptive practices

and violating advertisements, and reports a \$644 million year-over-year increase in marketing and sales expense driven mainly by professional services related to ongoing platform-integrity efforts. It does not isolate fake-copyright scams, total scam-related expense, victim loss or revenue from fraudulent ads.

This distinction matters because three different claims are often collapsed into one: what victims lost, what Meta earned from advertising, and what Meta spent or forgone through enforcement. Each requires a different dataset. No audited filing supplies the narrow breakdown.

Status	Claim or record	What can responsibly be said
Audited / established	Meta 2025 total revenue: \$200.966B. Public filing contains no scam-ad or copyright-pretext revenue line.	The denominator is known; the narrow revenue and loss quantities are unknown.
Platform-reported	Meta says it removed 159M scam ads and 10.9M scam-centre-linked accounts in 2025, plus >20M accounts impersonating large creators.	These are enforcement indicators under Meta’s definitions, not an audit of prevalence or economic harm.
Reuters-reported and disputed	Internal documents reportedly estimated about 10.1% of 2024 revenue—roughly \$16B—from ads for scams and prohibited goods, and about 15B high-risk scam ads served daily.	The estimate was broad, internal and unaudited. Meta called it rough and overly inclusive and said the true number was lower.
Pending civil allegation	Santa Clara County’s May 2026 complaint alleges about \$7B in annual revenue from advertising that exposes users to scams and describes a penalty-bid system for suspected advertisers.	Treat as an allegation in unresolved litigation, not a judicial finding and not a copyright-only figure.
Government concern	A bipartisan coalition of 42 state and territory attorneys general urged stronger advertiser vetting, human review and accountability for investment-scam ads in June 2025.	The letter documents regulator concern and requested changes; it does not independently audit the \$16B or \$7B figures.
Unknown	Meta’s direct cost, foregone revenue, liability and net loss specifically attributable to copyright-pretext impersonation.	No defensible public figure was located as of 10 August 2026.

Sources: Meta Platforms 2025 Form 10-K; Meta enforcement disclosures (2026); Reuters (6 November 2025); County of Santa Clara complaint and release (11 May 2026); NAAG coalition letter (June 2025).

10.1 ECONOMIC INCENTIVES AND THE EVIDENCE GAP

An ad auction can create incentive tensions even without proving intentional support for fraud. Platforms earn when advertisements are purchased; enforcement can reject spend, increase review cost and remove accounts; weak enforcement can impose victim, advertiser and trust costs elsewhere. Reuters’ reporting and Santa Clara County’s complaint allege more specific internal practices. Those allegations deserve scrutiny, but the evidence must be described at its procedural level.

Platform accountability should therefore focus on auditable questions: What share of suspicious-ad spend is refunded or rejected? How many advertisers are verified before spend? What happens below the automatic-ban threshold? How often are removed advertisers connected to replacement accounts? What is the time from report to durable disruption? How many legitimate advertisers or creators are wrongly removed and restored? Publishing those denominators would move the debate beyond uncheckable headline estimates.

FACT-CHECK VERDICT Do not write that Meta ‘lost \$16 billion’ or ‘earned \$16 billion from fake copyright scams.’ The \$16 billion figure is Reuters’ report of a disputed internal estimate covering broad scams and prohibited goods; the exact copyright-pretext share, Meta’s net benefit and Meta’s attributable loss are unknown.

11. COPYRIGHT, IMPERSONATION AND LEGAL-PROCESS ABUSE

11.1 THREE ROLES FOR COPYRIGHT

Role	Mechanism	Primary classification
Content copied for credibility	A false profile reproduces photographs, video, artwork, text or brand assets belonging to a creator or rightsholder.	Potential copyright infringement plus identity, trademark, passing-off, privacy/publicity, fraud or platform-rule issues
Real process abused	An actor submits a knowingly baseless or materially false notice, claim or counter-notice to remove content, redirect revenue, pressure a target or threaten account continuity.	Copyright-process abuse; possible statutory, contractual, fraud, extortion or platform consequences depending on law and facts
Fake copyright pretext	A forged strike, legal letter, rights-agent or platform-support message leads to a false login, file, call, payment or recovery route.	Social engineering, phishing, malware, impersonation or fraud using copyright language

Sources: *U.S. Copyright Office Section 512 Study (2020); YouTube Help; Government of Pakistan Copyright Ordinance and PECA; NCCIA identity-theft guidance.*

11.2 UNITED STATES NOTICE-AND-TAKEDOWN CONTEXT

Section 512 of the U.S. Copyright Act establishes notice-and-takedown and counter-notification processes associated with online-service-provider safe harbours. A compliant notice includes identification of the protected work and allegedly infringing material, contact information, specified statements and a signature. A counter-notice may expose personal contact information and consent to jurisdiction. That procedural seriousness is one reason scammers can make a forged notice feel urgent.

Section 512(f) addresses knowing material misrepresentations in notices and counter-notices, but the U.S. Copyright Office's 2020 study explains that remedies can be difficult in practice. Researchers should not label an ordinary mistake or disputed fair-use judgment "fraud" without evidence of knowledge and material misrepresentation. Nor should creators respond to a suspicious email by submitting a legal counter-notice before confirming that a real in-product case exists and considering privacy and legal consequences.

11.3 PAKISTAN CONTEXT

Pakistan's Copyright Ordinance 1962 governs copyright, while the Prevention of Electronic Crimes Act 2016, as amended, contains provisions relevant to electronic forgery, electronic fraud and unauthorized use of identity information. PECA also has an extraterritorial provision where conduct outside Pakistan has an effect on a person, property, information system or data in Pakistan. The National Cyber Crime Investigation Agency is the federal investigative body identified under the amended framework, and NCCIA's public identity-theft guidance expressly recognizes fake social accounts that impersonate a person. PTA directs online-fraud complaints to NCCIA.

Classification should remain fact-specific. A copied photograph may engage copyright; a cloned business name or logo may raise trademark or passing-off questions; false documents may involve electronic forgery; account takeover may involve unauthorized access; and a payment scheme may constitute electronic fraud. Victims should obtain qualified Pakistani legal advice for litigation, preservation demands or cross-border action.

SAFE RESPONSE TO A SUSPICIOUS COPYRIGHT MESSAGE Check the platform dashboard by opening the service directly—not through the message. Preserve the original message and link. Confirm the claimant and work. Do not share passwords, codes or remote access. Do not pay a private ‘agent’ to stop a strike. Escalate through the platform’s published route and obtain legal advice before filing a formal counter-notice.

12. EVIDENCE-BASED CASE STUDIES

12.1 COMPROMISED CREATOR CHANNELS: TRUST AS A RESALE ASSET

Google’s Threat Analysis Group documented campaigns targeting YouTube creators with cookie-theft malware. Compromised channels could be sold or repurposed for cryptocurrency scams, demonstrating why an established audience, posting history and authenticated session have market value. A stolen session can bypass the protection expected from a password change or second factor until the session is revoked. Google’s later device-bound-session work is designed to reduce the usefulness of stolen cookies.

Lesson: creator security is not only password security. Recovery email, delegated roles, active sessions, devices, browser tokens, downloaded sponsorship files and support workflows belong in the asset inventory. A copyright or partnership lure should be verified in-product before any file is opened or credential entered.

12.2 GENESIS MARKET: SPECIALIZATION OF THE ACCESS LAYER

Genesis Market separated theft from use. Malware-derived access packages could be purchased by downstream actors who did not compromise the computer themselves. The official seizure record supports the supply-chain model and the idea that a visible impersonation profile may be several steps removed from the original intrusion.

Lesson: marketplace inventory should not be multiplied by an advertised price to claim market revenue. Inventory, sale, successful login, downstream impersonation and victim loss are separate events with separate denominators.

12.3 VERIFTOOLS, ONLYFAKE AND SECONDEYE: SYNTHETIC IDENTITY AS A SERVICE

The VerifTools seizure, OnlyFake guilty plea and SecondEye prosecution show an enabling category spanning fabricated identity documents, account creation and attempts to circumvent online verification. SecondEye is particularly relevant to the author’s observation of advertised ban and unban services because public case material described sellers claiming that documents could assist people whose accounts had been banned or suspended.

Lesson: the defensible finding is the existence of an illicit supply service and documented intended uses. The evidence does not prove that every social platform accepted the documents, that every advertised country template worked or that every seller claiming “verification” is connected to these services.

12.4 YOUTUBE LLC V. BRADY: REAL-PROCESS ABUSE USED FOR EXTORTION

In 2019, YouTube sued Christopher Brady in the U.S. District Court for the District of Nebraska. YouTube alleged that Brady used false identities and fraudulent copyright notices against creators, then threatened additional strikes or account termination unless users paid. The case ended with a stipulated judgment and permanent injunction barring materially false notices and related conduct. The official case record is important because

it shows copyright-process abuse functioning as leverage against platform-dependent livelihoods, not merely as a mistaken takedown.

Lesson: preserve the actual notice, claimant identity, demand and platform history. The presence of an extortion demand and falsified identity transforms the evidentiary picture, but allegations should be distinguished from the final injunction and agreed disposition.

12.5 RECOVERY IMPERSONATION: THE SECOND VICTIMIZATION

FBI public-service announcements in 2025 and 2026 warn that scammers impersonate U.S. officials or recovery organizations, create fake personas and social pages, and contact people who have already lost money. One warning describes directing victims to Telegram. This is the recycling stage of the model: the first incident creates a list of distressed, motivated targets; the second actor promises restoration, then asks for fees, identity data or further transfers.

Lesson: incident response must protect the victim after the first report. Platforms and agencies should warn that officials do not privately demand cryptocurrency, fees, codes or remote access to recover funds. Researchers should code repeat contact and the source of victim targeting, because a recovery scam may reveal data sharing across supplier networks.

12.6 META’S ENFORCEMENT CONTROVERSY: SCALE, INCENTIVES AND PROCEDURAL STATUS

Meta’s platform disclosures establish a very large enforcement burden. Reuters’ reporting supplies a disputed internal revenue estimate, state attorneys general document regulatory concern, and Santa Clara County’s complaint places broad profit and enforcement allegations into litigation. None is interchangeable. Together they show why platform economics belongs in the study; separately they demonstrate why every assertion needs a status label.

Lesson: a responsible paper can investigate corporate incentives without presenting a complaint as a verdict or an internal estimate as an audited financial line. The unresolved research task is to obtain transparent denominators linking ad spend, detection confidence, refunds, repeat advertisers, user reports and durable removal.

13. IMPACT ON CREATORS, CONSUMERS, PLATFORMS AND SOCIETY

The economic transfer is only the visible core of the harm. Impersonation can interrupt income, destroy account history, confuse evidence of authorship, expose followers to fraud and make every authentic message less credible. A creator whose account is restored may still face lost sponsorships, search demotion, audience distrust and a renewed wave of fake “recovery” contacts. The term toxic impersonation is useful when it describes this compounding effect, but it should not replace measurable incident fields.

Stakeholder	Direct harm	Systemic harm	Useful metric
Creators and public figures	Account loss, diverted revenue, copied work, reputational damage, threats, recovery time	Withdrawal from public participation; reduced trust in authentic communication	Downtime; restored audience; verified interruption loss; recurrence; safety impact
Followers and consumers	Payment loss, credential theft, malware, identity compromise, emotional distress	Reduced trust in recommendations, charities, support and digital commerce	Gross paid; recovered; repeat contact; credential reset; complaint outcome

Stakeholder	Direct harm	Systemic harm	Useful metric
Brands and rightsholders	Counterfeit offers, customer confusion, copied campaigns, support burden	Dilution of authentic channels and higher enforcement cost	Incident rate; support contacts; conversion diversion; removal time
Social-media companies	Review, refund, account recovery, advertiser investigation, legal demands	Lower platform trust, regulator exposure and weaker ad/creator ecosystems	Time to detect; false-positive restoration; replacement rate; refund rate
Advertisers and intermediaries	Spend misdirection, brand-safety failures, chargebacks, mule-account exposure	Higher verification cost and reduced auction confidence	Beneficiary blocks; rejected spend; repeat advertiser linkage; chargebacks
Governments and financial institutions	Complaints, investigations, freezes, victim support and cross-border requests	Organized-crime finance, jurisdiction friction and public distrust	Preservation speed; freeze/recovery value; linked networks; case disposition
Scam-centre workers	Coercion, trafficking, violence, document confiscation and forced criminality in documented settings	A dual-victim problem that simple offender labels can obscure	Recruitment route; coercion indicator; referral to protection; organizer identification

13.1 PLATFORM HARM IS NOT A SINGLE LOSS LINE

Platforms can suffer support and enforcement costs, legal exposure, advertiser distrust and long-term degradation of user confidence. They can also receive advertising revenue before detection. Without internal cost allocation and scam-ad accounting, it is not possible to calculate net platform loss. Revenue foregone by rejecting a fraudulent advertiser is not the same as a cash loss, and a victim’s transfer should not be booked as the platform’s loss unless the platform reimburses it.

This is why the public debate should demand transparent operational metrics instead of an invented net number. A platform can publish scam-ad spend rejected before delivery, spend refunded after detection, victim reimbursements, account-recovery cost, report-to-action time, false-positive reversals and repeat-network reappearance without exposing sensitive detection systems.

14. PAKISTAN FOCUS AND COMPARATIVE RESEARCH GAPS

Pakistan is a strong setting for an original next phase because creators, small businesses and consumers operate across global platforms while complaints, payments and legal remedies cross jurisdictions. The country has applicable cybercrime and copyright law and public reporting channels, but the review did not locate a national, machine-readable annual series isolating social-media impersonation, copyright pretexts, account takeover, migration platform, payment rail and verified loss. That absence should be published as a finding, not filled with estimates imported from the United States.

A Lahore-based study can contribute globally if it uses an internationally comparable codebook. The research should include Urdu, English and Roman Urdu terms; document both local and international payment paths; record platform and NCCIA outcomes; and distinguish victim residence from the many other location signals. It should not label a host, seller or operator “Pakistani,” “Chinese,” “Indian” or otherwise based only on language, phone prefix or server geolocation.

Location field	Question answered	Common error
Victim location	Where was the affected person or organization?	Treating victim geography as offender geography

Location field	Question answered	Common error
Account registration signal	What region or data was associated with account creation?	Assuming registration proves current controller location
Login or device signal	Where did observed access appear to originate?	Ignoring VPN, proxy, compromised device or mobile routing
Phone-number registration	Where was the number issued or registered?	Treating a prefix or virtual number as nationality
Bank or wallet beneficiary	Which account or address received funds?	Equating a mule or exchange with the organizer
Domain and hosting	Where were registrar, DNS and server resources located?	Calling hosting location the operator's location
Marketplace language	Which language was used to market the service?	Inferring nationality or physical hosting from language
Workforce location	Where did contacting workers operate?	Failing to distinguish coerced workers from organizers
Organizer control	Where did the controlling decision-maker operate?	Stating control without financial, device, communication or adjudicated evidence

Sources: *Original attribution protocol informed by UNODC (2025, 2026), INTERPOL (2026), Europol (2025) and the cross-border enforcement records cited in this report.*

14.1 PROPOSED PAKISTAN RESEARCH QUESTIONS

36. Which identities are most frequently impersonated: creators, brands, public officials, platform support, financial services or recovery agents?
37. What share of verified incidents begins on one platform and migrates to another service, including Telegram, WhatsApp, email, phone or a stand-alone website?
38. How often does a copyright or account-policy pretext precede credential theft, malware delivery, a payment demand or a real false notice?
39. Which account-history and synthetic-verification signals appear in confirmed incidents, and which seller claims fail when checked against outcomes?
40. What are median report-to-acknowledgment, report-to-action, restoration and recurrence times across platforms and NCCIA referrals?
41. What are gross paid, recovered and net verified losses, kept separate from attempted amounts and creator interruption costs?
42. Which interventions produce durable disruption rather than profile replacement?

15. RECOMMENDATIONS

15.1 SOCIAL-MEDIA AND MESSAGING PLATFORMS

43. Publish separately defined metrics for impersonation, compromised accounts, scam advertising, fake support, copyright-tool abuse, repeat networks, user reports, proactive detection and restored false positives.
44. Place every copyright notice and account-policy action in a signed in-product case record. A user should never need to authenticate through a message link to inspect a strike or appeal.
45. Adopt passkeys or other phishing-resistant authentication, rapid session revocation, high-risk recovery review and device-bound sessions for creator, business and moderator accounts.

46. Expose meaningful account-age and significant rename history where safe, and require re-verification before a mature account makes high-risk identity, advertising or payment changes.
47. Detect copied profile media, near-identical biographies and cross-account asset reuse while preserving appeals for parody, fan pages, agents, shared brands and legitimate reuse.
48. Verify high-risk advertisers before spend, add human review for suspicious investment and celebrity/creator impersonation, and publish rejected, refunded and repeat-network ad metrics.
49. Share high-confidence domains, beneficiaries, wallets, devices and administrator clusters through lawful industry channels, with privacy controls and false-positive remediation.
50. Measure disruption durability: replacement time, migration, repeat-victim contact and common control—not removals alone.

15.2 REGULATORS, LAW ENFORCEMENT AND GOVERNMENTS

51. Standardize complaint fields for impersonated entity, platform, first contact, migration path, takeover status, synthetic identity, copyright pretext, payment rail, gross paid, recovered amount and case outcome.
52. Publish anonymized, machine-readable annual data with category definitions, missing-data rates and deduplication rules, including a Pakistan series capable of international comparison.
53. Use rapid preservation and lawful cross-border requests for account identifiers, ad buyers, domains, wallets, bank beneficiaries, login records and recovery changes before data expire.
54. Target organizers, access brokers, document services, money movement and common infrastructure rather than measuring success only by visible-profile removal.
55. Differentiate organizers from persons trafficked or coerced into scam-centre labour and route potential victims to protection.
56. Require large platforms to report scam-ad economics and appeal quality under consistent definitions without forcing publication of evadable detection thresholds.

15.3 CREATORS, BRANDS AND HIGH-RISK ORGANIZATIONS

57. Maintain an asset register covering official account IDs, domains, content masters, brand elements, recovery contacts, administrators, monetization services and third-party agencies.
58. Publish an official verification page listing real accounts and support addresses, and state that passwords, one-time codes, emergency payments and remote access will never be requested by direct message.
59. Use passkeys or hardware-backed MFA; secure recovery email and phone channels; restrict collaborator privileges; and review active sessions and delegated roles regularly.
60. Confirm copyright, verification, sponsorship and recovery messages inside the platform or through an independently obtained contact route before opening files, following links or sharing documents.
61. Preserve account IDs, full URLs, UTC timestamps, original messages, headers, link destinations, payment records, login alerts, case numbers and content ownership evidence before blocking or deleting.

62. Prepare a follower-warning template and an incident decision tree before a crisis. Recovery speed improves when responsibilities, counsel, payment contacts and platform routes are known in advance.

15.4 RESEARCHERS AND JOURNALISTS

63. Do not infer nationality from language, phone prefix, hosting geolocation or victim testimony alone; label each location signal and confidence.
64. Separate advertisements, observed transactions, verified delivery, seller receipts, victim payments, attempted losses and recoveries.
65. Archive evidence with hashes and timestamps, document inclusion criteria, and publish uncertainty and negative findings.
66. Do not republish active criminal links, seller handles, identity documents, stolen credentials or instructions that increase marketplace reach.
67. Treat a platform’s enforcement disclosure as a platform claim and a complaint as an allegation until adjudicated.

15.5 PAYMENT, ADVERTISING, HOSTING AND IDENTITY INTERMEDIARIES

68. Detect repeated beneficiaries, merchant identities and wallets linked to removed impersonation networks; preserve evidence and apply lawful holds quickly.
69. Add step-up checks when a beneficiary, advertiser or domain abruptly changes identity, geography, account ownership or high-risk product category.
70. Provide an authenticated emergency route for platforms and agencies to preserve or freeze funds while maintaining due process and restoration for false positives.
71. Share aggregate disruption results so researchers can measure migration rather than merely displacement to another provider.

16. MEASUREMENT FRAMEWORK FOR FUTURE FIELD RESEARCH

The next study should be prospective, incident based and preregistered. A twelve-month pilot could enrol creators, brands, investigators and support organizations in Pakistan, with a small comparison sample elsewhere. Each case should receive a stable research identifier and link platform, content, access, infrastructure, payment and complaint evidence without publishing the victim’s identity.

Sampling from only one source will bias the result. Marketplace observation overrepresents public sellers and advertisements; victim recruitment overrepresents recognized or harmful incidents; platform referrals reflect one company’s detection; agency data reflect reporting access and legal categories. The pilot should combine sources, record how each incident entered the study, and deduplicate by account ID, content hash, beneficiary, domain, device or administrator evidence.

Data block	Minimum fields	Verification rule
Incident	Research ID; first-contact UTC; claimed identity; pretext; platforms; migration; outcome	Contemporaneous capture or export plus researcher timestamp
Account	Stable platform ID; URL; creation/rename signals; followers; copied media; status	Platform-visible evidence; display name alone is insufficient
Content	Original source; publication time; licence/ownership; copied version; perceptual/cryptographic hash	Owner record and time-stamped comparison
Access	Login alerts; sessions; password/recovery changes; delegated roles; malware finding	Owner evidence, forensic record or platform case outcome
Authority/pretext	Copyright notice; support identity; document; sender; destination; demand	In-product case or preserved original message and metadata

Data block	Minimum fields	Verification rule
Infrastructure	Domain; registrar; DNS history; hosting ASN; TLS; redirects; app/bot identifiers	Time-stamped passive or lawfully obtained data; hosting kept separate from control
Payment	Rail; beneficiary; currency; requested; paid; recovered; wallet/receipt	Bank, wallet, receipt or verified complaint record
Location	Victim; account signal; login; phone; beneficiary; host; workforce; organizer	Every field tagged by evidence type and confidence
Enforcement	Report time; agency/platform; case ID; acknowledgment; action; restoration; recurrence	Platform or agency acknowledgment and archived status
Loss	Gross paid; recovered; net paid; interruption; remediation; attempted amount	Categories remain separate; assumptions and receipts documented

16.1 PROPOSED OUTCOME MEASURES

Outcome	Definition
Verified incidence	Number of deduplicated incidents meeting a published minimum evidence threshold within the sample and period
Net verified victim loss	Gross amount paid minus amount recovered, using transaction evidence
Report-to-action time	Elapsed time between verified report submission and first meaningful platform or agency action
Restoration time	Elapsed time until a legitimate account, content or monetization is restored
Replacement time	Elapsed time until the same network reappears using linked identity, content, administrator, domain or beneficiary evidence
Durable disruption rate	Share of acted-on networks with no linked reappearance during a defined follow-up period
False-positive restoration rate	Share of reviewed actions found erroneous and restored, with median restoration time
Migration rate	Share of incidents that move between platforms or communication layers before conversion
Repeat-victim contact rate	Share of victims contacted again by linked or recovery-themed actors during follow-up

16.2 CONFIDENCE AND PUBLICATION THRESHOLDS

Confidence	Minimum basis	Permitted wording
Confirmed	Transaction or platform/agency record plus stable identifiers and contemporaneous evidence	‘The incident involved...’ within the documented scope
Probable	Multiple independent signals with no material contradiction	‘Evidence strongly indicates...’ and list unresolved fields
Possible	One credible signal or victim report lacking independent verification	‘Reported or suspected...’; exclude from confirmed prevalence and loss totals
Advertisement only	Marketplace or seller claim without delivery or outcome proof	‘A service was advertised...’; never state that it worked
Unresolved allegation	Complaint, indictment or contested claim before disposition	‘Alleged...’; identify case and status

16.3 ETHICS AND DATA PROTECTION

72. Use informed consent and a clear withdrawal process for victim participants.
73. Collect the minimum personal data needed; separate identifiers from analysis records and encrypt both at rest and in transit.
74. Create a procedure for imminent threats, trafficking indicators, active account compromise and recoverable payments.
75. Do not purchase illegal access, impersonate victims, submit test notices, move criminal funds or interact in ways that create demand.
76. Obtain legal and institutional ethics review before covert observation, handling stolen data or publishing sensitive evidence.
77. Release an anonymized codebook, aggregate results, missing-data rates and methodology; use hashes or coded indicators rather than live credentials or criminal endpoints.

17. LIMITATIONS AND CONCLUSION

17.1 LIMITATIONS

78. This is a secondary-evidence working paper and conceptual framework, not a peer-reviewed prevalence survey, undercover market census or forensic audit of any platform.
79. Official complaint systems undercount incidents and are affected by recognition, access, missing fields, category design and reporting incentives.
80. Platform figures are self-reported and use definitions that are not fully comparable across companies or years.
81. Law-enforcement releases describe detected cases, seizures and selected operations; pending complaints and indictments are allegations.
82. The latest comparable full-year FTC, FBI and Meta data at the cut-off are for 2025. Partial 2026 enforcement announcements are not substituted for annual loss series.
83. No comparable public national loss series for the narrow category was located for Pakistan; U.S. or regional figures cannot be imported as a proxy.
84. Marketplace advertisements can be false, duplicated or recycled. No underlying coded field sample or verified transaction ledger was supplied for this edition.
85. The supplied Digital Fortress PDF omits a visible author line; the credit to Ans Ishfaq relies on matching contemporary publication profiles and should be checked against the final publisher or retail record.
86. The author's experience statement is self-reported and was not independently verified.

17.2 CONCLUSION

Social-media impersonation fraud is an economy of transferable trust. Established accounts, recognizable identities, copied expression, audience history, platform authority and plausible payment routes can each be stolen, purchased or fabricated. Marketplaces and messaging services connect specialized suppliers to operators; compromised accounts turn trusted audiences into distribution; synthetic documents attack verification; and manipulation converts an apparently official problem into credentials, control or money.

Copyright matters in this economy, but precision matters more. It supplies valuable content to copy and a real institutional language—claims, strikes, takedowns and counter-notices—that can be weaponized. Yet the underlying incident may be primarily account

compromise, identity misuse, phishing, fraud, extortion or organized criminal finance. A serious study records those acts separately.

The evidence supports two firm conclusions. First, the phenomenon is not merely a collection of isolated fake profiles. Access markets, document services, platform enforcement and international operations reveal specialization and industrial scale. Second, no authoritative public source measures the exact global loss or revenue of copyright-pretext impersonation. The responsible response is not to invent precision; it is to build the incident-level evidence needed to measure the problem.

Abdul Qudoos's strongest prospective contribution is therefore a transparent Pakistan-centred dataset connected to international definitions. If implemented with ethical safeguards, verified loss accounting and durable-disruption measures, that study could show how trust assets move across platforms, which interventions work, how victims are re-targeted and where complaint systems fail. That is new public value: a method others can inspect, reproduce and improve.

APPENDIX A. CLAIM AUDIT AND EVIDENCE MATRIX

Claim / metric	Value or status	Source class	Confidence	Critical caveat
U.S. social-media-contact loss, 2025	\$2.1B; 28% share in defined loss reports	FTC official statistics	High for reported category	Not global or impersonation-only; voluntary reports and shutdown gap
U.S. imposter-scam loss, 2025	\$3.5B across contact methods	FTC official statistics	High for reported category	Overlaps possible; do not add to social-media loss
IC3 complaints and losses, 2025	1,008,597; \$20.877B	FBI official report	High for reporting programme	Not prevalence; complaint and category overlap
Regional scam loss estimate, 2025	\$88.3B–\$114.1B	UNODC model	Moderate–high for stated region	All scams; methods and coverage differ
Genesis Market access inventory	>1.5M compromised computers; >80M credentials	DOJ action	High for authority-reported inventory	Not completed sales or impersonation cases
Synthetic identity services	VerifTools seizure; >10,000 OnlyFake documents in guilty plea	DOJ actions	High for case facts at stated status	Does not establish acceptance by every platform
Meta enforcement, 2025	159M scam ads; 10.9M scam-centre-linked accounts; >20M large-creator impersonators	Platform disclosure	Moderate–high for disclosed enforcement	Not audited prevalence, victim count or loss
Meta \$16B estimate	Reuters-reported internal 2024 estimate for broad scams and prohibited goods	Investigative reporting	Moderate for existence/context of reported documents	Disputed, unaudited and not copyright-specific
Meta \$7B allegation	Santa Clara County complaint alleges annual revenue tied to scam exposure	Pending complaint	High that allegation was filed; unresolved on merits	Not a finding and not copyright-specific
Telegram blocked communities, 2026	>22.5M displayed 10 Aug 2026	Dynamic platform counter	High for observed platform display	All abuse types; changes continuously; not a scam census
Exact global niche value	Not established	Cross-source assessment	High confidence in data gap	Requires verified, deduplicated transaction and loss data

APPENDIX B. IMPERSONATION INCIDENT RECORD

The following record is designed for a spreadsheet, case-management system or research database. One row should represent one deduplicated incident; repeating entities such as accounts, payments and reports belong in linked tables. Sensitive values should be encrypted or tokenized, and public extracts should replace identifiers with codes or hashes.

Field	Format / values	Required evidence
incident_id	Stable research code	Generated by research team; no personal identifier
source_route	victim / platform / agency / marketplace / researcher	Recruitment or referral record

Field	Format / values	Required evidence
first_contact_utc	ISO 8601 timestamp	Original message, export or contemporaneous capture
impersonated_entity_type	creator / brand / official / platform / recovery / other	Identity claimed in preserved evidence
initial_platform	Controlled vocabulary	Stable account or message identifier
migration_path	Ordered list of services/domains	Conversation export, URLs or redirect record
pretext_types	copyright / support / verification / investment / recovery / other; multi-select	Exact preserved wording
acts_observed	content_clone / fake_profile / ATO / phishing / malware / false_notice / payment; multi-select	Separate evidence for each act
account_ids	Linked entity table	Stable platform IDs and archived URLs
content_hashes	SHA-256 and/or perceptual hash	Original and copied files with ownership record
notice_case_id	Platform or legal reference	In-product notice, agency or court record
domain_or_bot_id	Linked infrastructure table	Time-stamped passive data
payment_request	Currency and amount	Preserved demand
gross_paid	Currency and verified amount	Receipt, bank or wallet record
recovered	Currency and verified amount	Reversal, freeze or return evidence
net_verified_loss	gross_paid – recovered	Calculated only after both fields are verified
creator_interruption_loss	Amount plus method	Documented baseline, period and assumptions
location_signals	Typed linked table with confidence	No nationality inference from a single signal
report_events	Agency/platform, UTC, case ID, action	Acknowledgment or status capture
recurrence	linked reappearance and UTC	Account/content/admin/payment linkage
confidence	confirmed / probable / possible / ad-only / alleged	Published threshold rules
consent_and_risk	coded status	Restricted participant record

APPENDIX C. PUBLIC INCIDENT-RESPONSE CHECKLIST

FIRST 30 MINUTES

87. Do not use links or phone numbers in the suspicious message. Open the official service directly and check the in-product case or security page.
88. Preserve the full message, sender, URL, account ID, timestamp, attachments and payment demand before reporting or blocking.
89. If account compromise is possible, use a known-clean device; change the primary password; revoke sessions; secure recovery email, phone and delegated roles; and enable a passkey or phishing-resistant MFA.
90. Contact the bank, payment provider or exchange immediately if money moved. Ask for a fraud hold or recall and preserve the case number.

FIRST 24 HOURS

91. Submit platform impersonation, compromise and—only where applicable—copyright reports through official forms. Record each case ID and submission time.

92. Warn followers through an unaffected official channel. State the exact fake account or tactic without amplifying criminal links.
93. Preserve ownership evidence for copied content and account history, including original files, publication dates and business records.
94. Report cybercrime in the relevant jurisdiction. In Pakistan, use NCCIA's official route; PTA's guidance directs online-fraud complaints to NCCIA.
95. Watch for recovery scammers. No genuine investigator or platform agent should require cryptocurrency, a password, one-time code or remote access to return funds or an account.

AFTER CONTAINMENT

96. Track platform action, restoration, payment recovery, new look-alike accounts and repeat victim contact for at least the defined follow-up period.
97. Review administrators, agencies, API access, ad accounts, browser sessions, recovery contacts and reused credentials.
98. Record gross paid, recovered and net loss separately, then document interruption and remediation costs with methods.
99. Update the public verification page and incident playbook based on what failed.

REFERENCES

Primary and official sources are prioritized. Platform sources are cited as platform-reported. Investigative reporting is retained where it describes non-public evidence and is labelled in the text. Access dates are included for dynamic pages.

Acharya, B., et al. (2024). The Imitation Game: Exploring Brand Impersonation Attacks on Social Media. 33rd USENIX Security Symposium. USENIX

Chromium Blog. (2024, April 2). Fighting cookie theft using device-bound sessions. Chromium

European Union Agency for Law Enforcement Cooperation. (2025). Steal, deal, repeat: How cybercriminals trade and exploit your data (IOCTA 2025). Europol PDF

Federal Bureau of Investigation. (2024, December 3). Criminals use generative artificial intelligence to facilitate financial fraud. IC3 PSA

Federal Bureau of Investigation. (2025, April 18). Scammers impersonate senior U.S. officials to target individuals. IC3 PSA

Federal Bureau of Investigation. (2026). 2025 IC3 Annual Report. IC3 PDF

Federal Bureau of Investigation. (2026, July 20). Scammers impersonating the FBI's Internet Crime Complaint Center to steal money from fraud victims. IC3 PSA

Financial Crimes Enforcement Network. (2025, October 14). FinCEN issues final rule severing Huione Group from the U.S. financial system. FinCEN

Google Threat Analysis Group. (2021, October 20). Phishing campaign targets YouTube creators with cookie theft malware. Google TAG

Government of Pakistan. (1962, as amended). Copyright Ordinance, 1962. Pakistan Code

Government of Pakistan. (2016, as amended). Prevention of Electronic Crimes Act, 2016. Pakistan Code PDF

INTERPOL. (2026). Global Financial Fraud Threat Assessment 2026. INTERPOL PDF

INTERPOL. (2026). Over 5,800 arrests, USD 293 million intercepted in global fraud bust. INTERPOL

Ishfaq, A. (2025). Digital Fortress: The Creator's Guide to Securing Content, Brand, and Legal Rights in the Online World [supplied PDF edition; attribution note in this report]. Publication profile

Meta Platforms, Inc. (2026). Annual Report on Form 10-K for the year ended December 31, 2025. SEC filing

Meta Platforms, Inc. (2026, January 28). Meta reports fourth quarter and full year 2025 results. SEC exhibit

Meta. (2025, April). Cracking down on spammy content on Facebook. Meta

Meta. (2026, March). Fighting scammers and protecting people with new technology and partnerships. Meta

Meta. (2026, March). Rewarding original creators on Facebook. Meta

National Association of Attorneys General. (2025, June 11). 42 state and territory attorneys general urge Meta to take action against investment scam ads. NAAG

National Association of Attorneys General. (2025). Letter to Meta regarding scam investment advertisements. Coalition letter PDF

National Cyber Crime Investigation Agency, Pakistan. (n.d.). Identity theft. NCCIA

Pakistan Telecommunication Authority. (2025). Where should I report incidents and complaints related to online fraud on social media platforms and the internet? PTA

Reuters. (2025, November 6). Meta is earning a fortune on a deluge of fraudulent ads, documents show. Reuters

Santa Clara County, Office of the County Counsel. (2026, May 11). County of Santa Clara files lawsuit alleging Meta knowingly facilitates and profits from scam ads. County release

Santa Clara County Superior Court. (2026). County of Santa Clara v. Meta Platforms, Inc. [Complaint; allegations unresolved as of the research cut-off]. Complaint PDF

Stajano, F., & Wilson, P. (2011). Understanding scam victims: Seven principles for systems security. Communications of the ACM, 54(3), 70–75. Author manuscript PDF

Telegram. (n.d.). Safety overview. Dynamic counter observed 10 August 2026. Telegram Safety

Telegram. (n.d.). Guidance for users covered by the EU Digital Services Act. Telegram DSA

- U.S. Copyright Office. (2020). Section 512 of Title 17: A Report of the Register of Copyrights. Copyright Office PDF
- U.S. Copyright Office. (n.d.). Section 512 Study. Copyright Office
- U.S. Department of Justice. (2023, April 5). Criminal marketplace disrupted in international cyber operation. DOJ
- U.S. Department of Justice. (2025, August 27). U.S. government seizes online marketplaces selling fraudulent identity documents used to bypass identity verification systems. DOJ
- U.S. Department of Justice. (2026, February). Creator of OnlyFake pleads guilty to selling more than 10,000 digital fake identity documents. DOJ
- U.S. Department of Justice. (2021). Two men charged with producing false identity documents and aggravated identity theft (SecondEye). DOJ
- U.S. Department of the Treasury. (2025, May 29). Treasury sanctions Funnall Technology for role in facilitating cyber scams. Treasury
- U.S. Department of the Treasury. (2026). National Money Laundering Risk Assessment. Treasury PDF
- U.S. Federal Trade Commission. (2026, April 27). Reported losses to scams on social media eight times higher than in 2020. FTC
- U.S. Federal Trade Commission. (2026, June 15). FTC data show people reported losing \$3.5 billion to imposter scams in 2025. FTC
- U.S. Government Publishing Office. (2019). YouTube, LLC v. Brady, No. 8:19-cv-00353 (D. Neb.). GovInfo case record
- United Nations Office on Drugs and Crime. (2025). Inflection Point: Global implications of scam centres, underground banking and illicit online marketplaces in Southeast Asia. UNODC PDF
- United Nations Office on Drugs and Crime. (2026, July). New UNODC report reveals scale of South-East Asia's ever more interconnected criminal economy. UNODC
- YouTube Help. (n.d.). Understand copyright strikes. YouTube Help
- YouTube Help Community. (2025). Phishing campaign using private video sharing. YouTube Help

SOURCE INTEGRITY NOTE Numbers and policies can change after the research cut-off. Readers should follow the linked primary record, confirm the current procedural status of litigation, and preserve access dates for dynamic platform pages.